UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,983	08/13/2001	Barry J. Gilhuly	1400-1072 P6	8317

54120 7590 05/13/2009

RESEARCH IN MOTION
ATTN: GLENDA WOLFE
BUILDING 6, BRAZOS EAST, SUITE 100
5000 RIVERSIDE DRIVE
IRVING, TX 75039

EXAMINER	
STRANGE, AARON N	

ART UNIT	PAPER NUMBER
2448	

NOTIFICATION DATE	DELIVERY MODE
05/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

portfolioprosecution@rim.com

Office Action Summary	Application No.	Applicant(s)	
	09/928,983	GILHULY ET AL.	
	Examiner	Art Unit	
	AARON STRANGE	2448	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/26/09*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *175-181,184-188,190-198,201-205,207-215,218-222,224 and 225* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *175-181,184-188,190-198,201-205,207-215,218-222,224 and 225* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. With regard to Applicant's assertion that "a Continuation-in-Part (CIP) application should be entitled to claim the benefit of an earlier non-provisional application if the CIP application otherwise complies with 35 U.S.C. §120 and 37 C.F.R. §1.78" (Remarks 21), the Examiner agrees.

However, as noted in the Office action of 11/26/08, the present application does not "otherwise comply with 35 U.S.C. §120 and 37 C.F.R. §1.78", since the earlier filed applications, International Patent Application No. PCT/CA00/01108 (filed Sep. 25, 2000), U.S. Patent Application No. 09/401,868 (filed Sep. 23, 1999), and U.S. Patent Application No. 09/087,623 (filed May 29, 1998) do not support the claims of the present application under the first paragraph of 35 U.S.C. §112, as required by 35 U.S.C. §120.

Accordingly, while the application may be a continuation-in-part of one or more of the prior filed applications, the claims of the present application are not entitled to an effective filing date as of the date any of the prior applications were filed. The effective filing date of all pending claims in the filing date of the present application, 8/13/2001.

Response to Arguments

2. Applicant's arguments with respect to claims 175-181, 184-188, 190-198, 201-205, 207-215, 218-222, 224 and 225 have been considered but are not persuasive.

3. With regard to claim 175, and Applicant's assertion that "Doonan's key server is not a computer associated with the user" (Remarks 25), the Examiner respectfully disagrees. As an initial matter, the term "associated with" is extremely broad, and requires little more than some identifiable connection between the associated items. IN this case, the fact that the user requests and obtains encryption keys from the "key server" certainly provides an association between the user and the key server. Furthermore, Doonan discloses that the "key server" is nothing more than a "software agent[]" (col. 3, ll. 9-12). One of ordinary skill in the art could have placed the software agent on any computer in the network, and would have recognized that systems generating the keys at various locations would have been nothing more than predictable variations of each other.

4. With regard to claim 175, and Applicant's assertion that "Doonan's key server does not create an encryption key in dependence on the user's interaction [with the computer at which the key is generated]" (Remarks 25), the Examiner agrees. However, this argument is moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 180, 181, 197, 198, 215 and 215 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

7. With regard to claims 180 and 181, the limitation “wherein sending the first encryption key further comprises generating a [public/private] key” is not described by the specification in the context of a symmetric key encryption scheme. Claim 175, from which claims 180 and 181 depend, requires generation of the first encryption key in dependence on the user's interaction with the computer system associated with the user. The specification only generates keys based on user interaction "[a]ccording to a symmetric key encryption scheme" (¶147). The specification describes public/private keys as being generated using an alternative “public key encryption scheme” (¶151). The specification fails to describe a scheme that generates public/private keys and also generates an encryption key in dependence on the user's interaction with a computer system.

8. Claims 197, 198, 214 and 215 contain a substantially identical limitation and are rejected under the same rationale.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 175, 178, 179-181, 184-188, 190, 192, 195, 196-198, 201-205, 207, 209, 212-215, 218-222 and 224 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile ("AirMobile Software of Lotus cc:Mail Wireless: Communication Server Guide") in view of Doonan et al. (US 6,807,277) further in view of Sussman (US 6,836,765).

11. With regard to claim 175, AirMobile discloses a method of redirecting data items from a messaging host system to a user's mobile device, comprising:

detecting a new data item for the user at the messaging host system (cc:Mail Post Office server) by the redirector host system (AirMobile Wireless for cc:Mail server) (new messages are received at the post office server, and detected by the AirMobile server)(pp. 25-26);

determining whether the new data item should be redirected from the redirector host system to the user's mobile device (AirMobile server checks download filters to determine whether to forward the message to the mobile device)(p. 26);

if the new data item should be redirected; and

transmitting the new data item from the redirector host system to the user's mobile device (messages passing the download filters will be sent to the wireless device)(p. 26).

While AirMobile teaches the use of a "secure and authenticated" channel (p. 25), it fails to specifically disclose that encrypting the messages prior to transmitting them via the channel using an encryption key generated at the computer system in dependence on the user's interaction therewith, or the computer system sending the encryption key and a decryption key to the redirector host and mobile device (via a secure connection).

Doonan discloses a similar system for transmitting electronic messages (Abstract). Doonan teaches use of a key server software agent that provides encryption keys to message “senders” and decryption keys to message “recipients” (col. 3, ll. 33-58), wherein the keys may be sent via secure connections (secure HTTP)(col. 3, ll. 40-42). Doonan discloses that the "senders” and “recipients” may be computers associated with users or software programs operating in an unattended "server mode" (col. 3, ll. 18-31). The addition of a key server software agent to AirMobile's system would have been advantageous since it would have provided encryption keys to the redirector host, decryption keys to the mobile device, and allowed messages to be encrypted to protect the messages from interception during transmission to the mobile device. However, Doonan fails to disclose that the encryption keys are generated in dependence on a user's interaction with the computer running the key server.

Sussman discloses a similar system for encrypting messages sent via the Internet (Abstract). Sussman discloses that it was well known in the art to generate

encryption keys depending on a user's interaction with the computer generating the keys (key generation may be based on mouse and keyboard input)(col. 9, ll. 4). This would have been an advantageous addition to the system disclosed by AirMobile and Doonan since it would have provided a relatively random seed for generation of the encryption keys, enhancing security of the messages.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the redirected messages prior to transmission to ensure that they were not intercepted by unauthorized recipients during transmission to the client, and to generate the encryption keys in dependence on the user's interaction with the computer generating the keys to improve the randomness of the key generation.

12. With regard to claim 178, Doonan further discloses that sending the first encryption key and sending the first decryption key further comprise generating a shared key (keys may be symmetric) (col. 9, ll. 54-61).

13. With regard to claim 179, Doonan further discloses generating the first encryption key and the first decryption key according to a symmetric key encryption scheme (keys may be symmetric) (col. 9, ll. 54-61).

14. With regard to claims 180 and 181, Doonan further discloses that the encryption/decryption keys comprise public and private keys (keys may be asymmetric) (col. 9, ll. 54-61).

15. With regard to claim 184, Doonan further discloses sending a second encryption key to the mobile device (a different encryption key is used by each sender, based on their credentials, so a different decryption key is needed for each message). (col. 3, ll. 32-45).

16. With regard to claims 185 and 186, Doonan further discloses that the encryption/decryption keys are a shared key generated in accordance with a symmetric key encryption scheme (col. 3, ll. 61-54; col. 9, ll. 48-53).

17. With regard to claims 187 and 188, Doonan further discloses that the encryption/decryption keys may be public/private keys (RSA is a public/private key encryption algorithm)(col. 9, ll. 54-61).

18. With regard to claim 190, AirMobile teaches that the mobile user can also transmit encrypted messages back to the network (p. 26-27). When considered in combination with the above noted teachings of Doonan, the combined references teach and/or suggest a system that system would encrypt any messages sent in reply to a

related message, transmit those replies back to the redirection server, decrypt the message and send it to the messaging host.

19. Claims 192, 195, 196-198, 201-205, 207, 209, 212-215, 218-222 and 224 are rejected under the same rationale as claims 175, 178, 179-181, 184-188 and 190, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

20. Claims 176, 193 and 210 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile ("AirMobile Software of Lotus cc:Mail Wireless: Communication Server Guide") in view of Doonan et al. (US 6,807,277) further in view of Sussman (US 6,836,765) further in view of Official Notice.

21. With regard to claim 176, while the system disclosed by AirMobile and Doonan shows substantial features of the claimed invention (discussed above), it fails to disclose establishing a serial connection between the redirector host system and the user's mobile device as the secure communications link.

The Examiner takes Official Notice that serial connections for transferring data between two computers were old and well known in the art at the time the invention was made. One of ordinary skill in the art would have been aware of serial connections and

would have recognized that a serial connection could have been used as the connection means, for example, when the mobile device is currently stored in a docking station.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a serial connection between the redirector host system and the user's mobile device, since serial connections, when available, are typically less expensive and more secure than wireless connections.

22. Claims 193 and 210 are rejected under the same rationale as claim 176, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

23. Claims 177, 194 and 211 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile ("AirMobile Software of Lotus cc:Mail Wireless: Communication Server Guide") in view of Doonan et al. (US 6,807,277) further in view of Sussman (US 6,836,765) further in view of Mansour et al. (US 2005/0278641).

24. With regard to claim 177, while the system disclosed by AirMobile and Doonan shows substantial features of the claimed invention (discussed above), it fails to disclose that establishing the secure communications link comprises using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

Mansour teaches that IMAP over SSL allows communications between a server and a client to be "fully encrypted" (¶29). Since AirMobile and Doonan use encryption to protect messages in transmission, and IMAP over SSL is a known encryption method, the use of IMAP over SSL in the combined system of AirMobile and Doonan would have been nothing more than a predictable variation of the encryption methods used by that system.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the well known IMAP over SSL protocol to “fully encrypt” messages transmitted between a server and a client.

25. Claims 194 and 211 are rejected under the same rationale as claim 177, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

26. Claims 191, 208 and 225 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile (“AirMobile Software of Lotus cc:Mail Wireless: Communication Server Guide") in view of Doonan et al. (US 6,807,277) further in view of Sussman (US 6,836,765) further in view of ARDIS (“ARDIS Begins Shipping New Lan-Based E-Mail Software; First Wireless Data Network to Offer Solution for Microsoft Mail and Lotusr (sic) cc:Mail Applications; Supports New Motorola Envoy 150 Wireless Communicator”).

27. With regard to claim 191, while the system disclosed by AirMobile and Doonan shows substantial features of the claimed invention (discussed above), it fails to specifically disclose that messages created at either the messaging host system or the mobile device share an electronic address as an originating address (i.e., the “from” address is the same whether the reply was created at the messaging host or the mobile device).

ARDIS discloses a publicly available software application called "Mail on the Run!", and further discloses that the software permitted a user of a mobile device to "wirelessly send, receive, store, forward and reply to messages on their corporate e-mail systems, retaining their LAN mailbox and ID” (p. 2, ¶1). This disclosure would have taught and/or suggested one of ordinary skill in the art to permit e-mail users to reply to messages from a mobile device in the same manner as though they had replied to the message from any other device in their "standard e-mail systems". “[R]etaining their LAN mailbox and ID” would have included using the same "from" address for the message, regardless of the device on which it was created.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the same originating address for a reply data item, regardless of the device on which the message was created since it would have allowed e-mail users to transparently access and use their e-mail from any device attached to the network.

28. Claims 208 and 225 are rejected under the same rationale as claims 191, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited art.

Conclusion

29. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AARON STRANGE whose telephone number is (571)272-3959. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Firmin Backer can be reached on 571-272-6703. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aaron Strange/
Examiner, Art Unit 2448